量子コンピュータ

著者名(日)	林,昌樹/勝浦,一雄
雑誌名	埼玉医科大学進学課程紀要
巻	8
ページ	1-5
発行年	2000-03-31
URL	http://id.nii.ac.jp/1386/00000117/

量子コンピュータ

林　　昌樹*・勝浦　一雄

Feynmanが初めて量子コンピュータのアイデアを発表したのは15年前のことである．このアイデアはその後いろいろな分野の理論家によって議論されてきたが，実現が大変難しく，理論家の思考実験の域をでていなかった．ところが最近量子コンピュータの基本となる量子ゲートが実験室で実証されてからにわかに注目を浴びるようになった．本稿では量子コンピュータの基本的な原理と現状について紹介する．

1　はじめに

近代的なコンピュータはTuring，Shannon等の理論的枠組みとvon Neumannによるプログラム内蔵方式のコンピュータの提案に基づいており，その最初のコンピュータが1950年に作られたEDVACであった．その後，トランジスタの発明，1960年代のトランジスタのIC化などの技術革新により，コンピュータの性能は急速に進歩し，現在のようなコンピュータ時代を実現するまでになった．

現在コンピュータはあらゆる場所で使われており，科学の進歩はコンピュータの性能の進歩と密接に関連するまでになり，ますますコンピュータの性能に対する社会の要求は厳しいものになってきている．そのようななかで現行方式のコンピュータの性能の限界も見え始めている．高度な集積化に伴う熱の発生の問題や，電子の速度が直接係わってくるような計算速度の限界などである．

このような限界をその枠組みから変えて打破しようとする試みの1つが量子力学的原理に基づくコンピュータ，すなわち量子コンピュータである．通常のコンピュータが電圧の高低で0と1を表現するのに対して，量子コンピュータでは例えば原子の励起状態と基底状態，素粒子の上下のスピン状態など，2準位系と呼ばれる系の2つの量子状態を0と1に対応させる．量子コンピュータでは可能な状態はこの2つの状態だけではなく，これらの状態の重ね合わせも許し，その1つ1つの状態に情報を載せ，計算処理を行なうことができる．n個の素子（原子）があれば少なくとも2^nの同時計算（並列処理）が行なえ，高速な演算速度が期待される．

実際，量子コンピュータを使えば離散対数問題や整数の素因数分解問題のようないわゆるNP完全問題が，従来のコンピュータよりはるかに少ないステップ数で確率的に解けることが証明されている［1］．

最近トラップされたイオンや，量子電気力学的共振器の中に置かれた原子と光に関する実験などで，量子コンピュータを構成する基本的な論理回路を構築できることが実証された［2］−［3］．このような基本的な論理回路を組み合わせることにより，原理的にはコンピュータ内で行われるあらゆる論理演算を遂行する回路が作成できることから，量子コンピュータの構想がにわかに現実味を帯びてきた．

量子力学の原理をコンピュータの世界に持ち込んだとき，どのようなことがおきるかを最初に考察したのはFeynmanである［4］−［5］．ここではFeynmanに従って量子コンピュータにおける基本的論理回路である，制御(CONTROLLED) NOT，2重制御（CONTROLLED CONTROLLED) NOTなどの可逆論理回路をまず紹介し，その後量子コンピュータについてその原理や問題点等を述べる．

*東京薬科大学生命科学部生命物理科学教室

2　可逆論理回路

従来の von Neumann 型コンピュータは数字や情報を 0 と 1 からなる 2 進数で表わし，この 2 進数を一定の手順に従って変換し，さまざまな演算を行っている．この演算の基礎となっているものが Boole 代数と呼ばれるものである．この代数によればこれらの変換は全て NOT および AND または OR と呼ばれる 2 種の論理回路（ゲート）の組み合わせで実現できることが分かっている．ゲートは入力と出力を持ち，入力の組み合わせで出力が一義的に決まる．入力と出力の関係を表に表したものを真理値表と言う．表 1 に AND，OR，NOT の真理値表を示す．

表 1　基本ゲートの真理値表

AND

入力		出力
a	b	c
0	0	0
0	1	0
1	0	0
1	1	1

OR

入力		出力
a	b	c
0	0	0
0	1	1
1	0	1
1	1	1

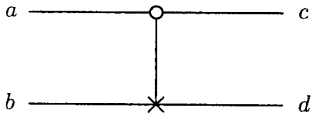
NOT

入力	出力
a	b
0	1
1	0

これらのゲートのうち AND と OR は 2 個の入力と 1 個の出力をもつ．従って，入力された情報の内 1 つはこのゲートを通ることにより失われることになり，不可逆なゲートである．一方，NOT では失われる情報はなく，可逆的なゲートとなっている．

量子コンピュータの場合，後で述べるように演算は量子状態に施されるユニタリー変換のことであり，この変換は可逆なので，不可逆なゲートは使えない．AND や OR に代る論理的に可逆なゲートとしては，Toffoli の提案した制御 NOT（図 1），2 重制御 NOT（図 2）がある［6］．

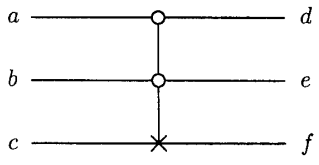
図 1



a	b	c	d
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

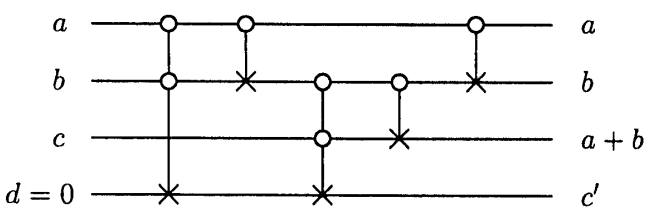
制御 NOT は 2 つの入力 a，b と 2 つの出力 c，d をもつ．a と c は常に同じ値をもち，出力 d をコントロールする役目をする．出力 d は $a=1$ のとき，$d=$NOT b，$a=0$ のとき $d=b$ のように変化する．このとき $d=a$ XOR b（$\equiv a \oplus b$）となっていることが真理値表より分かる．2 重制御 NOT は 3 つの入力 a，b，c と 3 つの出力 d，e，f をもつ．$a=d$，$b=e$ であり，a，b は出力 f をコントロールする役目をもち，$a=b=1$ の場合のみ，$f=$NOT c となり，それ以外は $c=f$ となる．これらのゲートが可逆であることは自明であろう．以上の 2 種のゲートを適当に組み合わせることにより，コンピュータ上で行われるさまざまな演算を実現することができる．図 3 にコンピュータ上で加算を行うための回路，いわゆる全加算器を 2 個の 2 重制御 NOT と 2 個の制御 NOT を使って実現している例を示す．ここで a，b は加数，被加数の任意の桁における数，c は前の桁からの繰り上がりの数，c' は加算する桁における繰り上がりの数を表す．

図 2



a	b	c	d	e	f
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

図 3



このような可逆論理回路は熱の発生を 0 にすることができる．AND ゲートのような不可逆ゲートの場合，先にも述べたように情報が失われ，そ

の時のエントロピー変化は ln 2 で，これに伴い温度 T で $kT\ln 2$ の熱が発生する［7］−［8］．論理的に可逆なゲートを使えばエントロピー変化がなく，原理的にはコンピュータのエネルギー消費を0にすることができるわけである．

上記の2種のゲートを粒子のスピンや光子の偏光などの量子力学に従う2準位系によって構成したものが量子コンピュータである．

3　量子コンピュータ

量子コンピュータでは通常のコンピュータ（以下古典コンピュータと呼ぶ）の0と1に対応するものとして2準位系の2つの量子状態を用いる．今，状態を $|0\rangle$，$|1\rangle$ のように記述すると，可能な状態 ψ はこれらの2つの状態の重ね合わせ，すなわち

$$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle \tag{1}$$

と表せる．ここで α，β は $|\alpha|^2+|\beta|^2=1$ を満たす複素数である．

古典コンピュータにおける計算は0と1で表わされた情報を別の0と1の列に変換する作業であったが，量子コンピュータにおいてはこれは α と β の変換，すなわち量子状態間の遷移に相当する．数学的にはこのような状態間の遷移はユニタリー変換と呼ばれる行列で表わすことができ，2準位系の場合のユニタリー変換は2行2列の行列となる．前述の NOT ゲートをユニタリー行列で表すと

$$\mathrm{NOT}=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} \tag{2}$$

となる．このユニタリー行列を量子力学でよく用いられる生成・消滅演算子で表してみよう．消滅演算子とは状態 $|1\rangle$（$=(0,\ 1)^{\mathrm{T}}$）を状態 $|0\rangle$（$=(1,\ 0)^{\mathrm{T}}$）に，状態 $|0\rangle$ を0に変換する演算子で，行列で表わせば

$$a=\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix} \tag{3}$$

である．生成演算子は逆に状態 $|0\rangle$ を状態 $|1\rangle$ に，状態 $|1\rangle$ を0に変換する演算子で，行列で表わせば

$$a^{\dagger}=\begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix} \tag{4}$$

である．ここで†はエルミート共役を表わす．これらの演算子を用いると NOT は

$$\mathrm{NOT}=a+a^{\dagger} \tag{5}$$

と表すことができる．また制御 NOT：$A_{a,b}$ の場合は

$$A_{a,b}=a^{\dagger}\ a\ (a+b^{\dagger})+aa^{\dagger} \tag{6}$$

のように表される．ここで，a，b は制御 NOT の2つの入力（量子状態）a，b に対応する消滅演算子である（混乱する恐れはないと思うので，演算子と入力を同じ文字で表わすことにする）．これが制御 NOT になっていることは次のように考えれば容易に分かる．右辺の最初の項 $a^{\dagger}\ a$ は入力 a が $|1\rangle$ のときのみ1となり，それ以外は0となるので，$a=|1\rangle$ の状態を選び出す．このとき $b+b^{\dagger}$ は入力 b に対する NOT 演算子として働く．同様に2重制御 NOT：$A_{ab,c}$ を演算子で表せば

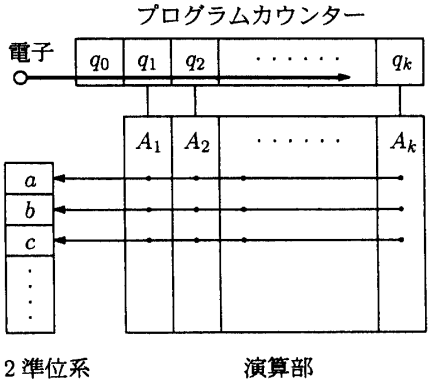
$$A_{ab,c}=1+a^{\dagger}\ ab^{\dagger}\ b\ (c+c^{\dagger}-1) \tag{7}$$

となる．前述の全加算機を制御 NOT，2重制御 NOT の演算子で表せば

$$M=A_{a,b}A_{b,c}A_{bc,d}A_{a,b}A_{ab,d} \tag{8}$$

となる．この演算子は右から順に $A_{ab,d}$，$A_{a,b,}\cdots$ を状態 a，b，c，d に施すことを意味する．このような演算を実際の2準位系を用いて実現するにはどのようにすればよいのだろうか．

図4



量子力学では状態 ψ の時間発展は系のハミルトニアンを H，初期（$t=0$）状態を ψ_0 とすると次のように表される．

$$|\psi\rangle = e^{-iHt}|\psi_0\rangle \tag{9}$$

ある時間 t における指数因子 e^{-iHt} が所定の演算に対応するようなハミルトニアン H を持つ系があれば，そのような系を使って演算が実現できる．この指数因子を展開すると

$$e^{-iHt} = 1 - iHt - H^2t^2/2 - \cdots \tag{10}$$

ここでHの高次の項は作用を繰り返し行うことを意味する．実行したい演算を

$$M = A_kA_{k-1}A_{k-2}\cdots A_2A_1 \tag{11}$$

とする．ここで，図4に示すように，実際に演算 M の対象となる n 個の2準位系 a，b，c，…とは別に A_i から A_k までの演算の進行を制御する働きを持つプログラムカウンターと呼ぶ $k+1$ 個の2準位系を用意する（古典計算機ではプログラムカウンターは次に計算機が実行する命令が格納されている番地を指し示すもので，プログラムの実行を制御する上で重要な役割を果たす）．プログラムカウンター i と演算 A_i はある種の相互作用で連結されているとしよう．ここではFeynmanに従ってプログラムカウンターの中を電子が移動する状況を考え，プログラムカウンター i に電子が存在している状態を $|1\rangle_i$，存在しない状態を $|0\rangle_i$ とする．これらの状態に対する消滅演算子を q_i と書き，次のようなハミルトニアンを考える

$$\begin{aligned} H &= \sum_{i=0}^{k-1} q_i^{\dagger}{}_{+1} q_i A_{i+1} + complex\ \ cojugate \\ &= q_1^{\dagger}\ q_0 A_1 + q_2^{\dagger}\ q_1 A_2 + \cdots + q_k^{\dagger}\ q_{k-1} A_k \\ &\quad + q_0^{\dagger}\ q_1 A_1^{\dagger} + q_1^{\dagger}\ q_2 A_2^{\dagger} + \cdots + q^{\dagger}{}_{k-1} q_k A_k^{\dagger} \end{aligned} \tag{12}$$

はじめに電子はプログラムカウンター0に存在しているとし，ハミルトニアン H を1回作用させると，上式の右辺の2行目，第1項（$q_1^{\dagger}\ q_0A_1$）の寄与により，電子はプログラムカウンター0からプログラムカウンター1に移動し，この際 n 個の2準位系 a，b，c，…には A_1 の演算が施される．ハミルトニアンのその他の項には電子の存在しない場所の消滅演算子が含まれているため，演算には寄与しない．時間発展の指数因子 e^{-iHt} の展開式中には H の2次の項が含まれていることに注目してもう1度ハミルトニアンを作用させると，前と同様にして上式の右辺の2行目，第2項（$q_2^{\dagger}\ q_1A_2$）の寄与により，電子はプログラムカウンター1からプログラムカウンター2に移動し，n 個の2準位系には先ほど A_1 の演算に引き続いて A_2 の演算が施される．ハミルトニアン H が何回か繰り返し作用した後，プログラムカウンター k の状態が $|1\rangle_k$ になっていれば n 個の2準位系には演算 $M = A_kA_{k-1}A_{k-2}\cdots A_2A_1$ が施されたことになる．ハミルトニアン H の3行目の項はすぐに分かるようにプログラムカウンター中を電子が逆行する場合に相当する．仮にプログラムカウンター i で電子が逆行し，プログラムカウンター $i-1$ に移動したとすると n 個の2準位系には演算 $A_i^{\dagger}\ A_i = 1$ が施されることになり，直前の演算が取り消される．つまり電子がプログラムカウンター中のどこにいるかで演算がどこまで為されたかが一意的に決まるわけである．

以上がFeynmanの量子可逆弾動コンピュータと呼ばれるもののおおよその動作原理である．量子コンピュータはこの他，Deutschを始めとする何人かの物理学者がいくつかモデルを考案し，その計算論的性質を研究している［9］－［10］．

4　おわりに

前節のような量子コンピュータで実際に計算を行なうためには，計算手順すなわちハミルトニアンのプログラム法，計算結果の読取り方法，プログラムカウンターと各計算ステップの連係方法など解決しなければならない数多くの問題がある．また，たくさんのゲートを組合わせた大規模な量子コンピュータの場合，莫大な数の重ね合わせ状態のコヒーレンスを維持するためにコンピュータは外界から厳しく隔離されていなければならないが，そのようなことは大変困難なことである．重ね合わせの係数が連続的な複素数値をとることから，わずかな誤差が累積する問題なども指摘されており，大規模な量子コンピュータの実現を疑問視する研究者もいる[11]．一方，量子コンピュータにおいて基本的なゲートの働きをするトラップされたイオンなどにみられる「エンタングルド状態」や，NP完全問題の解法などは量子力学の観測問題と関係しており，この方面の知見を深めるの

に役立つものと見られている．またPenroseやDonaldは量子コンピュータと，人工知能，神経回路，脳科学，知性との関係について論じており，この方面の研究は幅広い広がりを見せている[12]－[13]．

参考文献

[1] P.W. Shor, Proc. of the 35th Annual Symposium on the Foundation of Computer Science, IEEE Computer Society Press, Los Alamitos, Calif., 116-123(1994).

[2] C. Monroe, D. Meekhof, B. King, W. Itano, D. Wineland, Phys. Rev. Lett. **75**, 4714(1995).

[3] Q. Turchette, C. Hood, W. Lange, H. Mabushi, H. J. Kimble, Phys. Rev. Lett. **75**, 4710(1995).

[4] R. P. Feynman, Int. J. Theor. Phys. **21**, 467-488(1982).

[5] R. P. Feynman, Found. Phys. **16**, 507-531(1986).

[6] T. Toffoli, Math. Syst. Theory **14**, 13-23(1981).

[7] R. Landauer, IBM J. Res. Develop. **5**, 183-191(1961).

[8] R. W. Keyes, Proc. IEEE **69**, 267-278(1981).

[9] D. Deutsch, Proc. Roy. Soc. London **A 400**, 97-117(1985).

[10] D. Deutsch, R. Jozsa, Proc. Roy. Soc. London **A 439**, 553-558(1992).

[11] S. Haroche, J-M Raimond, Phys. Today **49**, 51-52(1996).

[12] R. Penrose, *The Emperor's New Mind Concerning Computers, Minds and the Laws of Physics*, Oxford Univ. Press, Oxford(1989).

[13] M. J. Donald, Proc. Roy. Soc. London **A 427**, 43-93(1990).